PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-184756
(43)Date of publication of application : 09.07.1999

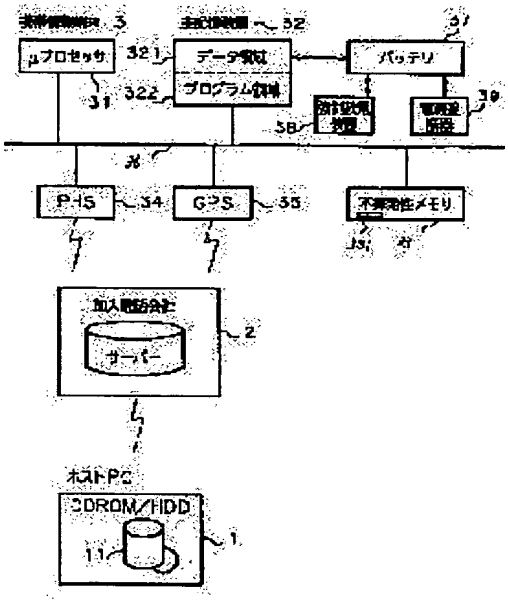
(51)Int.Cl. G06F 12/14

(21)Application number : 09-357756
(22)Date of filing : 25.12.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : NOSE MASAKI
NUMAJIRI YUTAKA

(54) SECURITY CONTROL METHOD IN PORTABLE INFORMATION TERMINAL AND SYSTEM THEREFOR AND RECORDING MEDIUM FOR PROGRAMMING AND RECORDING THE SAME METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the leakage or illegal use of information by operating and managing the security function of a portable information terminal only by access from a personal computer without operating it by the portal information terminal itself.
SOLUTION: A portable information terminal 3 receives a request for access to security related information from a host equipment 1, certifies identification information recorded in a recording medium 11 provided on the host equipment 1 and a unique identification number (non-volatile recording medium 33) provided on the portable information terminal, and permits or rejects the access according to the certified result, and communicates it to the host equipment 1. Thus, access is performed from the outside by using this so that the deletion of the secret information of a portable information terminal equipment whose location is unknown due to robbery, the report of a robber's information, and transition to a state incapable of use can be attained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－184756

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ ３２０Ｄ

審査請求　未請求　請求項の数33　ＯＬ　（全 22 頁）

(21)出願番号　特願平9－357756

(22)出願日　平成９年(1997)12月25日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　野瀬　正毅
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(72)発明者　沼尻　裕
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

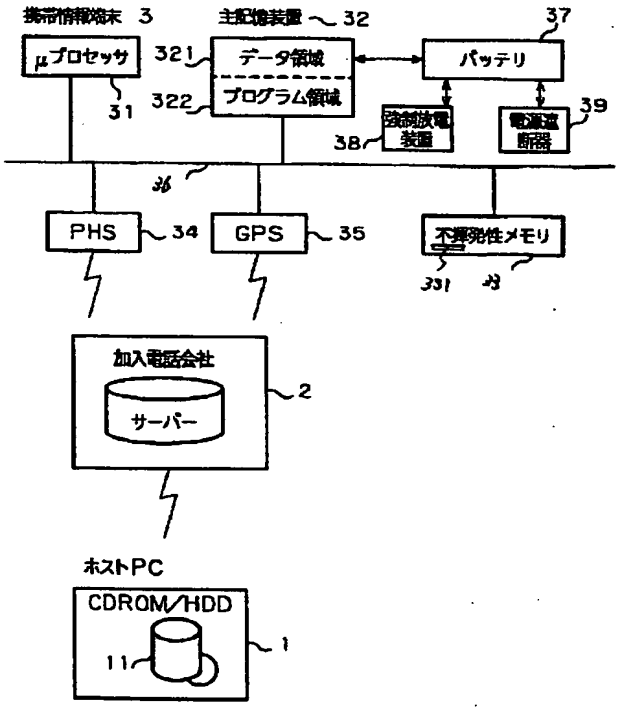
(74)代理人　弁理士　大胡　典夫　（外１名）

(54)【発明の名称】　携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記録媒体

(57)【要約】

【課題】　本発明は、携帯情報端末のセキュリティ機能をその携帯情報端末自身で操作することなく、パーソナルコンピュータからのアクセスでのみ操作管理することにより、情報の漏洩、不正使用を防止するとともに、セキュリティ機能の充実をはかることを課題とする。

【解決手段】　本発明は、携帯情報端末３において、ホスト機器１からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体１１に記録されている識別情報と携帯情報端末が持つユニークな識別番号（不揮発性記録媒体３３）との認証を行ない、認証結果によっては、アクセスを許可もしくは拒否し、ホスト機器に通知する。このことを利用し外部からアクセスすることで盗難による所在不明な携帯情報端末の機密情報削除、盗難者情報の通知、使用不能状態への移行を行なう。



1

【特許請求の範囲】

【請求項１】　自身でアクセスできない穏蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末であって、携帯情報端末毎付されるユニークな識別情報と同一、もしくは対応する識別情報を持つホスト機器によってのみ上記機密情報ファイルのアクセスを許可することを特徴とするセキュリティ制御方法。

【請求項２】　携帯情報端末において、ホスト機器からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体に記録されている識別情報と携帯情報端末が持つユニークな識別番号との認証を行ない、認証結果によっては、上記のアクセスを許可もしくは拒否し、ホスト機器に通知することを特徴とするセキュリティ制御方法。

【請求項３】　携帯情報端末が持つ識別情報と同一、もしくは対応する識別情報を持つホスト機器から一定期間以上アクセスが無い場合に不正使用と判断することを特徴とする請求項２記載のセキュリティ制御方法。

【請求項４】　初期設定時において隠蔽された情報ファイルと同一もしくは共通のデータが格納され、携帯情報端末からアクセス可能な開放された情報ファイルと、携帯情報端末が持つ記録媒体に記録された穏蔽された機密情報ファイルの内容を比較し、その結果によっては不正使用と判断することを特徴とする請求項２記載のセキュリティ制御方法。

【請求項５】　不正使用である旨の通知をうけたとき、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項３または４記載のセキュリティ制御方法。

【請求項６】　携帯情報端末からの要求に従い、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項５記載のセキュリティ制御方法。

【請求項７】　不正使用である旨の通知をうけたとき、携帯情報端末が持つ記録媒体のバックアップのための電源を強制放電し、記録情報を消去することを特徴とする請求項３または４記載のセキュリティ制御方法。

【請求項８】　携帯情報端末からの要求に従い、携帯情報端末が持つ記録媒体のバックアップのための電源を遮断し、記録情報を消去することを特徴とする請求項７記載のセキュリティ制御方法。

【請求項９】　ホスト機器が携帯情報端末に対して通信回線を介して接続要求を発し、所有者からの通信であるか否かを上記識別情報の比較によつて認証を行ない、通信回線を介して到来するコマンドを受信してそのコマンドに従うセキュリティを実行することを特徴とする請求項１記載のセキュリティ制御方法。

【請求項１０】　加入している電話会社に対し、加入通信機器を含む携帯情報端末の発信位置情報を要求し、当該携帯情報端末の通信機が使用中であれば受信局の特定

2

により概略使用位置情報を得ることを特徴とする請求項９記載のセキュリティ制御方法。

【請求項１１】　個々にユニークな識別情報が付され、自身でアクセスできない穏蔽された機密情報ファイルを含む記録媒体を持つ携帯情報端末と、上記識別情報に対応する識別情報を含み、上記携帯情報端末と協動して上記機密情報ファイルのアクセスを行なうホスト機器が通信回線を介して接続されて成ることを特徴とする携帯情報端末におけるセキュリティ制御システム。

【請求項１２】　上記携帯情報端末は、識別番号があらかじめ書き込まれ、自身でアクセスできない不揮発性メモリと、上記識別情報と同一、もしくは対応する識別情報を持つホスト機器によってアクセスされ、自身でアクセスできない穏蔽された機密情報ファイルを含む記録媒体とを具備することを特徴とする請求項１１記載のセキュリティ制御システム。

【請求項１３】　記録媒体の記憶内容のバックアップを行なうバックアップ電源を更に具備することを特徴とする請求項１１記載のセキュリティ制御システム。

【請求項１４】　外部からの指示によりバックアップ電源の遮断を行なうか、強制放電を行なう電源制御装置を更に具備することを特徴とする請求項１１記載のセキュリティ制御システム。

【請求項１５】　ホスト機器との通信を確立する移動電話を更に具備することを特徴とする請求項１１記載のセキュリティ制御システム。

【請求項１６】　ホスト機器からの要求に基づき発信位置を通知するＧＰＳ受信機を更に具備することを特徴とする請求項１５記載のセキュリティ制御システム。

【請求項１７】　上記ホスト機器は、携帯情報端末が持つ識別情報と同一もしくは対応する識別情報を持ち、携帯情報端末と協動して携帯情報端末が持つ機密情報ファイルをアクセスするプログラムが格納される記録媒体を具備することを特徴とする請求項１１記載のセキュリティ制御システム。

【請求項１８】　自身でアクセスできない穏蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末において用いられ、外部接続されるホスト機器から上記機密情報ファイルに対するアクセス要求を受け付けるステップと、ホスト機器の識別情報を読み込むステップと、携帯情報端末が持つ識別情報と上記ホスト機器の識別番号を比較して同じ、もしくは対応関係にあるか否かを判断するステップと、上記比較の結果によっては携帯情報端末の機密情報ファイルへのアクセスを許可、もしくは拒否することをホスト機器に通知するステップとがプログラムされ記録されるコンピュータ読み取り可能な記録媒体。

【請求項１９】　穏蔽された機密情報ファイルのアクセス要求を受信するステップと、携帯情報端末からの要求であったときそのアクセスを拒否し、否であったときホ

3

スト機器からの要求であることを確認し、識別情報のマッチング検査を行ないホスト機器から機密情報ファイルのアクセスを実行するステップとがプログラムされ記録される請求項１８記載のコンピュータ読み取り可能な記録媒体。

【請求項２０】　携帯情報端末に記録された、前回ホスト機器によりアクセスされた時刻情報を読み取るステップと、現在日時と上記時刻情報を比較し、所定の時間以上アクセスがなかったことを検査するステップと、検査の結果によりアクセス時刻情報を更新、もしくは不正使用と判断して外部へ通知するステップとがプログラムされ記録される請求項１８記載のコンピュータ読み取り可能な記録媒体。

【請求項２１】　穏蔽された機密情報ファイルの内容を参照するステップと、初期設定時において隠蔽された情報ファイルと同一もしくは共通のデータが格納され、携帯情報端末からアクセス可能な開放された情報ファイルの内容を参照するステップと、穏蔽された情報ファイルと開放された情報ファイルの対応する項目の内容の一致を検査するステップと、検査結果によっては不正使用と判断し、外部へ通知するステップとがプログラムされ記録される請求項　１８記載のコンピュータ読み取り可能な記録媒体。

【請求項２２】　不正使用を検知することにより起動され、携帯情報端末の記録媒体のバックアップ電源を遮断すべく指示を発するステップがプログラムされ記録される請求項２１記載のコンピュータ読み取り可能な記録媒体。

【請求項２３】不正使用を検知することにより起動され、携帯情報端末が持つ記録媒体のバックアップ電源に対し強制放電を指示するステップがプログラムされ記録される請求項２１記載のコンピュータ読み取り可能な記録媒体。

【請求項２４】　不正使用の通知を受けフラグをセットするステップと、通信コネクションを確立することにより起動され、フラグを参照するステップと、フラグがセットしていたとき、穏蔽された機密情報ファイルに格納されたアドレス先に、開放された情報ファイルの内容を電子メールで送付するステップとがプログラムされ記録される請求項２１記載のコンピュータ読み取り可能な記録媒体。

【請求項２５】　不正使用を検知することにより起動され、割り込み禁止状態に設定するステップと、携帯情報端末が持つ記録媒体の全てのファイル、もしくは事前に指定したファイルの内容を強制削除するステップとがプログラムされ記録される請求項２１記載のコンピュータ読み取り可能な記録媒体。

【請求項２６】　携帯情報端末の表示画面に開放された情報ファイルの内容を表示するステップと、その情報ファイルに対する変更要求を受け付け、エディタを起動して編集処理を行なうステップと、変更要求がないとき、あるいは編集処理終了後にその表示を閉じるステップとがプログラムされ記録される請求項１８記載のコンピュータ読み取り可能な記録媒体。

4

【請求項２７】　ホスト機器が携帯情報端末に対し通信回線を介して接続要求を発することにより起動され、所有者からの通信であるか否か上記識別情報のマッチング検査によつて認証するステップと、通信回線を介してコマンドを受信し、セキュリティ機能を起動するステップと、コマンドに従うセキュリティを実行するステップとがプログラムされ記録されるコンピュータ読み取り可能な請求項１８記載の記録媒体。

【請求項２８】　セキュリティモードにあることを検査するステップと、リモートロックを行なうコマンドを受信するステップと、携帯情報端末をロックするステップとがプログラムされ記録される請求項　２７記載のコンピュータ読み取り可能な記録媒体。

【請求項２９】　通信回線を介して警告音を発するコマンドを受信するステップと、携帯情報端末から警告音の発生を指示するステップとがプログラムされ記録される請求項２７記載のコンピュータ読み取り可能な記録媒体。

【請求項３０】　携帯情報端末にＧＰＳ受信機が装備されていることを検査するステップと、ＧＰＳ受信機を介して現在位置を通知するステップとが更にプログラムされ記録される請求項２７記載のコンピュータ読み取り可能な記録媒体。

【請求項３１】　データを消去するコマンドを受信するステップと、携帯情報端末が持つ記録媒体に記録されてある情報を消去するステップとが更にプログラムされ記録される請求項２７記載のコンピュータ読み取り可能な記録媒体。

【請求項３２】　識別情報のマッチングによる認証に従い、携帯情報端末に対するプログラムの再インストールを許可するステップが更にプログラムされ記録される請求項２７記載のコンピュータ読み取り可能な記録媒体。

【請求項３３】　加入している電話会社に対し、加入通信機器を含む携帯情報端末の発信位置情報を要求するステップと、当該携帯情報端末の通信機が使用中であれば受信局の特定により概略使用位置情報を得るステップとがプログラムされ、記録される請求項１８記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記録媒体に関する。

【０００２】

【従来の技術】半導体技術の進歩に伴い携帯情報端末が普及してきた。携帯情報端末はパーソナルユースがほと

んどであり、従って、業務情報の他にプライバシー情報も扱うことが多く、収納データに対するセキュリティ保護が望まれていた。

【０００３】また、携帯情報端末は、社内や自宅で使用する他、携帯して外で使用することができることから盗難や紛失する可能性もある。しかしながら、情報漏洩を防ぐための手段や盗難を抑止するための手段はほとんど講じられていないのが現状である。携帯情報端末は、その性格上廉価構成をとることがのぞまれ、従って、基本性能ではないセキュリティのために特別な機能を装置に付加することは困難であった。

【０００４】

【発明が解決しようとする課題】電子手帳から発展した携帯情報端末は共用することを前提としていないため、ほとんどがセキュリティ機能を装備していない。また、パーソナルコンピュータから発展し、小型化された携帯情報端末は、ブートメディアを使用して立ち上げることでパスワードを回避して使用することが可能である。

【０００５】一方、ネットワークコンピュータやＰＨＳ内蔵の情報端末が登場したが、パスワードによるセキュリティのみで、能動的に情報漏洩を防ぐ機能は用意されていない。将来的にデファクトスタンダードになると予測されるハンドヘルドコンピュータが１９９６年末米国で発売され、１９９７年夏から国内でも販売が開始されたが、その中に十分なセキュリティ機能は搭載されていない。この種携帯情報端末に格納された情報は、他の全ての携帯情報端末によりアクセスすることができるため、有効なセキュリティ機能の実現が困難であった。

【０００６】携帯情報端末は、基本的に単体で用いることは少なくパーソナルコンピュータと連係して使用することが多い。そこで、携帯情報端末のセキュリティ機能をその携帯情報端末自身で操作することなく、パーソナルコンピュータからのアクセスでのみ操作管理することにより、情報の漏洩、不正使用を防止するとともに、セキュリティ機能の充実をはかった携帯情報端末におけるセキュリティ制御方法ならびに装置及び同方法がプログラムされ記録される記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の携帯情報端末におけるセキュリティ制御方法は、自身でアクセスできない穏蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末であって、携帯情報端末毎付されるユニークな識別情報と同一、もしくは対応する識別情報を持つホスト機器によってのみ上記機密情報ファイルのアクセスを許可することを特徴とする。また、携帯情報端末において、ホスト機器からセキュリティ関連情報のアクセス要求を受け、ホスト機器が持つ記録媒体に記録されている識別情報と携帯情報端末が持つユニークな識別番号との認証を行ない、認証結果によっては、上記のアクセスを許可もしくは拒否し、ホスト機器に通知することも特徴とする。

【０００８】本発明のセキュリティ制御システムは、個々にユニークな識別情報が付され、自身でアクセスできない穏蔽された機密情報ファイルを含む機密情報ファイルを含む記録媒体を持つ携帯情報端末と、上記識別情報に対応する識別情報を含み、上記携帯情報端末と協動して上記機密情報ファイルのアクセスを行なうホスト機器が通信回線を介して接続されて成ることを特徴とする。

【０００９】本発明の記録媒体は、自身でアクセスできない穏蔽した機密情報ファイルを含む記録媒体を持つ携帯情報端末において用いられ、外部接続されるホスト機器から上記機密情報ファイルに対するアクセス要求を受け付けるステップと、ホスト機器の識別情報を読み込むステップと、携帯情報端末が持つ識別情報と上記ホスト機器の識別番号を比較して同じ、もしくは対応関係にあるか否かを判断するステップと、上記比較の結果によっては携帯情報端末の機密情報ファイルへのアクセスを許可、もしくは拒否することをホスト機器に通知するステップとがプログラムされ記録されることを特徴とする。

【００１０】上述した携帯情報端末におけるセキュリティ制御方法ならびに装置及び同方法がプログラムされ記録される記録媒体を用い、不正使用を検知し、また、電源遮断による情報漏洩の防止、あるいは強制放電による情報漏洩防止、電子メールによる自動情報通知、更には、ホスト機器からのアクセスによるセキュリティリモートコントロール、リモートロック、リモート警告音発生、リモート所在通知、リモートデータ消去、リモートアクセス認証、携帯情報端末盗難時に加入電話会社による位置情報を取得することにより、充実したセキュリティ機能を実現できる。

【００１１】

【発明の実施の形態】図１は本発明の実施形態を示すブロック図である。図において、符号１は、ホストとなるパーソナルコンピュータであり、電話会社２が管理する回線経由で携帯情報端末３が接続される。

【００１２】携帯情報端末は、制御中枢となるマイクロプロセッサ３１、プログラム乃至データが格納される記録媒体３２、不揮発性メモリ３３、通信媒体となるＰＨＳ３４、あるいはＧＰＳ３５がバス３６を介して共通接続される。記録媒体３２は、データ領域３２１とプログラム領域３２２から成り、各領域に割り付けられるデータ、プログラムについては図２で詳述する。不揮発性メモリ３３には携帯情報端末の識別情報３３１が記録される。３７は記録媒体３２の記憶内容保持のために使用される電源バッテリであり、更に、ある条件の下で強制放電させる強制放電装置３８、電源供給を遮断する電源遮断器３９が組込まれている。

【００１３】図２は、図１における記録媒体に割り付けられ格納されるデータやプログラムを記録媒体上に展開

して示した図である。

【００１４】データ領域３２１には、所有者の氏名、住所、電子メールアドレス、電話番号、パースワード等の機密情報が格納される穏蔽したい機密情報ファイル３２１１、対応するパーソナルコンピュータに接続される毎に更新され、携帯情報端末からは変更できない接続情報３２１２、使用者の氏名、住所、電話番号、電子メールアドレス等リードライト可能な個人情報ファィル３２１３がデータ領域に割り付けられ記録される。

【００１５】また、プログラム領域３２２には、不正使用検知プログラム３２２１，３２２２、電源遮断プログラム３２２３、個人情報表示＆変更プログラム３２２４、記録媒体強制削除プログラム３２２５、インタネット接続検知プログラム３２２６、自動情報通知プログラム３２２７、パスワード要求プログラム３２２８、強制情報削除プログラム３２２９、リモートロックプログラム３２３０、リモート警告音発生プログラム３２３１、リモート所在通知プログラム３２３２、リモートデータ消去プログラム３２３３、リモートアクセス認証プログラム３２３４、インストール管理プログラム３２３５、機密情報ファィル変更プログラム３２３６がそれぞれ割り付けられ記録される。

【００１６】不正使用検知プログラム３２２１は、接続履歴が一定期間以上更新されなかったときに不正使用であると識別するために用意される。不正使用検知プログラム３２２２は、穏蔽した機密情報ファイル３２１１と個人情報ファイル３２１３の内容を比較し、不一致のときに不正使用であると識別するために用意される。

【００１７】電源遮断プログラム３２２３は、不正使用の通知を受けると電源遮断装置３９を用いて携帯情報端末３の記録媒体３２の記憶保持のために使用される電源供給を遮断して情報を消去するために用意される。個人情報表示＆変更プログラム３２２４は、個人情報ファィル３２１３の内容を携帯情報端末３の画面に表示し、また、変更要求を受け付け、個人情報ファィル３２１３の内容を変更するために用意される。記憶媒体強制削除プログラム３２２５は、携帯情報端末３の記憶媒体３２に記憶されるデータを強制的に削除するために用意される。

【００１８】インタネット接続検知プログラム３２２６は、ネットワークプロトコル、あるいはネットワークデバイスドライバ等通信リソースを管理し、電子メールの送信が可能か否かを関しするために用意される。自動情報通知プログラム３２２７は、インタネットを用いて穏蔽した機密情報ファイル３２１１に記録したアドレスへ、個人情報ファイル３２１３の情報を電子メールによって自動送信するために用意される。

【００１９】パスワード要求プログラム３２２８は、携帯情報端末３がレジューム等休止の状態から復帰する際に、パスワード入力を要求し、不一致の場合に稼動状態

に移行させないために用意される。強制情報削除プログラム３２２９は、不正使用の通知を受けた場合にバッテリの強制放電装置３８を用い記録媒体３２の記憶保持のために使用されるバッテリ３７を強制放電し、情報を消去するために用意される。

【００２０】リモートロックプログラム３２３０は、遠隔地にあるホストパーソナルコンピュータ１より、後述するセキュリティリモートコントロールプログラム１１５の要求を受け、携帯情報端末３の電話受信機能以外の入出力機能をロックするために用意される。リモート警告音発生プログラム３２３１は、遠隔地にあるホストパーソナルコンピュータ１より、セキュリティリモートコントロールプログラム１１５の要求を受け、音声や警告音を発生するために用意される。リモート所在通知プログラム３２３２は、遠隔地にあるホストパーソナルコンピュータ１より、セキュリティリモートコントロールプログラム１１５の要求を受け、携帯情報端末３に接続するＧＰＳ３５より現在地を求めホストパーソナルコンピュータ１へ通知するために用意される。

【００２１】リモートデータ消去プログラム３２３３は、遠隔地にあるホストパーソナルコンピュータ１より、セキュリティリモートコントロールプログラム１１５の要求を受け、携帯情報端末３の記録媒体３２の情報を強制削除するために用意される。リモートアクセス認証プログラム３２３４は、遠隔地にあるホストパーソナルコンピュータ１より、セキュリティリモートコントロールプログラム１１５を介してアクセス要求を受けた場合、要求に含まれる後述する識別情報と携帯情報端末３の不揮発性メモリ３３に内蔵の識別情報３３１のマッチングをとり、不一致の場合にはセキュリティリモートコントロールプログラム１１５の要求を拒否するために用意される。

【００２２】インストール管理プログラム３２３５は、携帯情報端末３にプログラムをインストールする際に使用されるインストーラで、識別情報と識別情報３３１のマッチングをとり、不一致の場合にはインストールを拒否するために用意される。機密情報ファィル変更プログラム３２３６は変更要求に含まれる後述する識別情報と携帯情報端末３にある識別番号３１３のマッチングをとり、一致したときに穏蔽した機密情報ファイル３２１１の内容を読み書きするために用意される。

【００２３】ホストパーソナルコンピュータ１は、ＣＤ－ＲＯＭもしくはハードディスク等の記録媒体１１を有し、ホストパーソナルコンピュータ１にユニークな識別番号１１１が記録される他、記録媒体３２に含まれる穏蔽した機密情報ファイル３２１をリードライトするためのアクセスプログラム１１２、記録媒体１１に含まれる識別情報１１１と携帯情報端末３の識別情報３３１とのマッチングをとり、不一致のときにはアクセスを拒否する認識プログラム１１３、対応する携帯情報端末３と接

続したときにその携帯情報端末３にある接続履歴情報３２２を更新する接続情報更新プログラム１１４、ＰＨＳ、ＧＰＳ等無線電話による通信媒体を介して携帯情報端末３にアクセスし、携帯情報端末３が持つリモートセキュリティ機能を制御するセキュリティリモートコントロールプログラム１１５、携帯情報端末３にソフトウェアをインストールする際に使用され、識別情報１１１と識別情報３３１のマッチングをとって不一致のときにインストールを拒否するインストーラ１１６、加入電話会社２の当該サーバにアクセスし、加入電話が使用中である場合には使用位置情報をアクセスして表示する位置情報取得プログラム１１７が割り付けられ記憶される。

【００２４】図３～図２２は本発明実施形態の動作を説明するために引用したフローチャートであり、それぞれが本発明により用意される各プログラムの実行手順を示す。

【００２５】以下、図３～図２２に示すフローチャートを参照しながら、図１，図２に示す本発明実施形態の動作について詳細に説明する。

【００２６】まず、携帯情報端末３の立ち上げから説明する。電源ＯＦＦ状態または、休止状態にある携帯情報端末３を稼動状態に移行するためには、パスワード要求プログラム３２２７が割り込み禁止状態となっているときに携帯情報端末３を起動する必要がある。携帯情報端末３が持つ入力装置を介して入力されたパスワードを、穏蔽した機密情報ファイル３２１１に記録されたパスワードと比較し、一致したときに優先度を元に戻して稼動状態へ移行する。パスワードが一致しなかつた場合は、優先度を元に戻してレジューム状態に移行する。

【００２７】ここで、穏蔽した機密情報ファイル３２１１の変更操作について図４に示すフローチャートを参照しながら説明する。穏蔽した機密情報ファイル３２１１は、携帯情報端末３から直接読み書きを行なえないような細工をしてある。所有者は、ホストパーソナルコンピュータ１から、携帯情報端末３にある不揮発性メモリ３３に内蔵された識別情報３３１と一致する識別情報１１１を持つ記憶媒体１１に割り付け格納済みの、穏蔽した機密情報ファイルのアクセスプログラム１１２を起動する。ここで、ホストパーソナルコンピュータ１と接続された携帯情報端末３は、機密情報ファイル変更プログラム３２３６を起動して上述した機密情報ファイルアクセスプログラム１１２の要求に含まれる識別情報１１１と携帯情報端末の不揮発性メモリ３３に記録されてある識別情報３３１の内容を比較（ステップＳ３）し、一致すれば隠蔽した機密情報ファイルアクセスプログラム１１２の変更内容入力受付ルーチンを起動し、使用者に変更内容の入力を促す。変更内容が入力されると、機密情報ファイル変更プログラム３２３６は、穏蔽した機密情報ファイル３２１１の変更処理（ステップＳ４）を行なう。

【００２８】ホストパーソナルコンピュータ１からのセキュリティ機能制御について図３に示すフローチャートを用いて説明する。ホストパーソナルコンピュータ１から携帯情報端末３のセキュリティ関連プログラム３２２１～３２３６を起動するとき、認識プログラム１１３により識別情報１１１と携帯情報端末３が持つ識別情報３３１の一致を確認（ステップＳ３）する。ここで一致が認められたときに要求のあったセキュリティ関連プログラムを起動（ステップＳ４）し、不一致であればセキュリティ機能関連の制御を拒否（ステップＳ５）する。

【００２９】次に、本発明の特徴の一つである接続履歴情報による不正使用の検知操作について図５に示すフローチャートを参照しながら説明する。接続履歴更新プログラム１１４は、ホストパーソナルコンピュータ１と携帯情報端末３が接続されたときに呼び出され、上述した認識プログラム１１３をコールして識別情報１１１と識別情報３３１の一致確認を行なう。ここで一致が認められたときに携帯情報端末３の記録媒体３１に格納される接続履歴情報ファイル３２１２を更新する。不正使用検知プログラム３２２１は、システム稼動時におけるトリガを利用して起動（ステップＳ１）され、接続履歴情報ファイル３２１２を参照し、現在日時と前回のアクセス日時を比較（ステップＳ３）して一定時間以上更新されなければ不正に使用されていると判断（ステップＳ４）する。

【００３０】一方、個人情報の矛盾による不正使用の検知について図６に示すフローチャートを参照しながら説明する。携帯情報端末３は上述した起動時等におけるトリガを利用して個人情報表示＆変更プログラム３２２７を起動する。このプログラム３２２７では、容易に表示情報を変更できるように、情報変更画面を設ける。不正な使用者がこの情報を変更した場合、携帯情報端末３の穏蔽した機密情報ファイル３２１１の内容との矛盾が生じる。これによって不正使用を検知する。通常、正規の利用者が穏蔽した機密情報ファイル３２１１の内容を変更した場合には、携帯情報端末３と対をなす記録媒体１１に格納された機密情報ファイル更新プログラム１１４を用いる。

【００３１】次に、本発明の特徴の一つである電源遮断による情報消去により情報漏洩を防止するための方法について、図７、図８に示すフローチャートを参照しながら述べる。図７に示すフローチャートにおいて、上述した不正使用検知プログラム３２２１あるいは３２２２により不正使用が通知（ステップＳ７１）されると、電源遮断プログラム３２２３は、電源遮断装置３９を制御して携帯情報端末３の記録媒体３２における記憶保持のための電源を遮断（ステップＳ７２）し、情報の消去をはかる。

【００３２】一方、図８に示すフローチャートにおいて、ステップＳ８１で不正使用が通知されると、記憶媒

体強制削除プログラム３２２５により優先度を最高レベルに設定して割り込み禁止とし（ステップＳ８２）、携帯情報端末３の記録媒体３２のファイルの全てを強制削除、あるいは事前に指定したファイルのみ強制削除する（ステップＳ８３）ことも考えられる。

【００３３】次に図９に示すフローチャートを参照しながら、本発明の特徴の一つである強制放電による情報漏洩防止方法について詳述する。不正使用検知プログラム３２２１、あるいは３２２２により不正使用が検知されることにより強制情報削除プログラム３２２９がコール（ステップＳ９１）される。このとき、強制情報削除プログラム３２２９は、バッテリ強制放電装置３８をコントロール（ステップＳ９２）することにより、携帯情報端末３の記録媒体３１の記憶内容保持のために供給されているバッテリ３１を強制放電し、情報を消去する。

【００３４】ところで、個人情報の表示＆変更プログラム３２２４は、携帯情報端末３の表示画面に公開された情報ファイルの内容を表示し、その情報ファイルに対する変更要求を受け付ける。そして、変更要求を受け付けるアイコンもしくはボタン等を使用者が操作したかチェックし、読み書き可能な個人情報ファイル３２１３を変更するためのエディタを展開する。このエディタを使用して編集処理を行ないエディタを閉じることにより本処理を終了する。変更要求がないとき、あるいは編集処理終了後にその表示を閉じる。

【００３５】次に、本発明の特徴の一つである不正使用者情報の電子メールによる通知について、図１０に示すフローチャートを参照しながら説明する。まず、不正使用検知プログラム３２２２により不正使用が検知され、このことが通知されると、不正使用であることを示すフラグをＯＮする（ステップＳ１０１）。後述するインタネット接続を検知する方法により接続が通知されると、インタネット接続検知プログラム３２２６が起動（ステップＳ１０２）され、インタネット接続検知プログラム３２２６は電子メール送出可能であることを検知すると先のフラグを確認（ステップＳ１０３）し、フラグがＯＮしていることにより、電子メールによる自動情報通知プログラム３２２７をコールする。自動情報通知プログラム３２２７は、秘蔽した機密情報ファイル３２１１に記録された本来の所有者のアドレスに対し、個人情報ファイル３２１３の内容を電子メールで自動送信する（ステップＳ１０４）。このとき、メールの送信を携帯情報端末保持者に通知しない。このことにより、本来の所有者は盗難者が入力した個人情報を知ることができる。

【００３６】インタネット接続を通知する方法は図１１にフローチャートで示されている。即ち、携帯情報端末３のダイヤルプロパティを設定する際、コネクションを確立した後、インタネット接続検知プログラム３２２６へ通知するように自動設定（ステップＳ１１１）する。そして、通信プロトコルを実現するプログラムにおいて

コネクションの確立を検出し、その旨通知（ステップＳ１１２，Ｓ１１３）するものである。

【００３７】次に、パスワード要求プログラム３２２８による、携帯情報端末３が休止状態から復帰するときのパスワードブロック動作について説明する。携帯情報端末３は、パワーセーブのため、一定時間アクセスがない場合レジューム状態を継続する機能を標準で持つ。この状態から復帰する際、パスワード要求プログラム３２２８を起動してパスワードの入力を要求する。不一致の場合は稼動状態に移行させることはない。

【００３８】次に、本発明の特徴の一つであるリモートアクセス認証方法について図１２に示すフローチャートを参照しながら説明する。ＰＨＳ３４等を介し、携帯情報端末３のリモートセキュリティ関連プログラム３２３０．３２３１，３２３２が、ホストパーソナルコンピュータ１のセキュリティリモートコントロールプログラム１１５からアクセス要求を受信した場合（ステップＳ１２１）、その要求に含まれる識別情報１１１（ステップＳ１２２）と不揮発性メモリ３３に登録されてある識別情報３３１とのマッチング（ステップＳ１２３）をとり、不一致の場合にはセキュリティリモートコントロールプログラム１１５の要求を拒否する。一致した場合には当該プログラムを起動（ステップＳ１２４）する。

【００３９】セキュリティリモートコントロールにつき、図１３～図１７を参照しながら説明する。まず、リモートロックから説明する。リモートアクセス認証プログラム３２３４によりリモートロックプログラム３２３０がコールされると、携帯情報端末３の電話受信機能以外の入出力機能のロック、アンロックを行なう。

【００４０】即ち、図１３、図１４のフローチャートにおいて、まず、リモートアクセス認証（図１３）がなされる。具体的には、携帯情報端末３に対して通信回線を介して外部から接続（ステップＳ１３２）を行ない、識別情報による所有者からの通信であるか否かの認証チェック（Ｓ１３２）が行なわれる。ここで、一致が確認されてアクセスが許可されると、通信回線からコマンドを受け付け（ステップＳ１３３）、セキュリティ機能を起動（ステップＳ１３４，Ｓ１３５）する。

【００４１】更に図１４のフローチャートに移行して、セキュリティモードにあるか否かがチェック（ステップＳ１４１）され、通信回線経由でリモートロックを行なうコマンドを受けたか否かをチェック（ステップＳ１４２，Ｓ１４３）する。そしてそのコマンドに従い携帯情報端末３をロック、もしくはアンロック（ステップＳ１４４）する。

【００４２】図１５はリモート警告音発生方法についてその制御手順がフローチャートで示されている。リモートアクセス認証プログラム３２３４からリモート警告音発生プログラム３２３１がコールされると、盗難を通知する音声や警告音を発生させる。まず、セキュリティモ

13

ードになっているか検査（ステップＳ１５１）され、通信回線経由で受信したコマンドをチェック（ステップＳ１５２，１５３）し、警告音発生を指示するコマンドであったときに携帯情報端末３から警告音を発生（ステップＳ１５４）させるものである。尚、この状態でレジューム状態に移行することはできない。

【００４３】図１６は、リモート所在地通知方法を実現するプログラムの動作手順をフローチャートで示したものである。ＧＰＳレシーバ３５を装備した携帯情報端末３において、リモートアクセス認証プログラム３２３４からリモート所在地通知プログラム３２３２がコールされると、ＧＰＳを介して現在地が求められ、ＰＨＳ３４等通信機器を介してホストパーソナルコンピュータ１へ携帯情報端末３の位置情報を通知するものである。

【００４４】リモート所在地通知プログラム３２３２は、セキュリティモードにあるか否かチェック（ステップＳ１６１）し、更に携帯情報端末３にＧＰＳ３５が装備されているかチェック（ステップＳ１６２）し、いずれも成立したときに、ＧＰＳによる現在位置を通信回線経由で得、その情報をホストパーソナルコンピュータ１へ通知（ステップＳ１６３）する。

【００４５】図１７は、リモートデータ消去方法を実現するリモートデータ消去プログラムの動作手順をフローチャートで示したものである。リモートアクセス認証プログラム３２３４からリモートデータ消去プログラム３２３３がコールされると、携帯情報端末３が持つ記録媒体３２に格納してある情報が強制削除される。

【００４６】リモートデータ消去プログラム３２３４は、まず、携帯情報端末３がセキュリティモードにあるか否かをチェック（ステップＳ１７１）し、通信回線経由で受信したコマンドの解析（ステップＳ１７２，Ｓ１７３）を行ない、データを消去すべきコマンドであったときに、指定された範囲のデータを消去（ステップＳ１７４）する。

【００４７】一方、携帯情報端末３にプロクラムを再インストールすることにより、セキュリティ機能が回避されることを防ぐためにインストール管理プログラム３２３５が用意される。インストール管理プログラム３２３５は、識別情報のマッチングがとれたときのみ、再インストールを許可し、セキュリティ機能の継続した実現をはかる。

【００４８】図１８は、無線電話会社により位置情報を得る方法をフローチャートで示したものである。ホストパーソナルコンピュータ１は、自身で持つ位置情報取得プログラム１１７に従い、加入先電話会社に対し加入通信機器、即ち、ここではＰＨＳ３４を含む携帯情報端末３の発信位置情報を要求する。ここで携帯情報端末３の通信機能が作動中であれば、受信局の特定によりおおまかな使用位置の特定がなされ、所有者に通知されるものである。

14

【００４９】具体的には、加入先電話会社に対して携帯情報端末が盗難にあつた旨連絡が入る（ステップＳ１８１）ことから処理が開始され、携帯情報端末３に対して通信回線を介して外部から接続（ステップＳ１８２）がなされる。このことにより、使用した中継アンテナの位置情報を電話会社が取得（ステップＳ１８３）し、中継アンテナのサービス範囲情報が電話会社から所有者に対して通知（ステップＳ１８４）される。ここで、所有者は、警察に連絡するか否か決断（ステップＳ１８５）し、場合によつてはその情報を伝達（ステップＳ１８６）することになる。

【００５０】尚、上述した実施形態では、ハンドヘルドコンピュータ、ウォレットパーソナルコンピュータ、ＰＤＡにＰＨＳを内蔵した携帯情報端末をホストパーソナルコンピュータに接続したもののみ例示したが、これに限定されるものではなく、ノートＰＣや、スケジューリングの機能を持つ時計や家電製品、あるいは将来、通信ネットワークに車が接続されるようになった場合、車のセキュリティに特に有効となるものである。

【００５１】以上説明のように本発明は、通信機能を持つ携帯情報端末において、ホストとなるパーソナルコンピュータと協動することにより、携帯情報端末が盗難にあつた場合の機密情報の漏洩防止、使用停止、所在確認を行なうものである。また、加入電話会社との連係により、盗難にあつた携帯情報端末の所在を特定することができるものである。

【００５２】

【発明の効果】以上説明のように、本発明は、携帯情報端末のセキュリティ機能を携帯情報端末自身で操作することなく、ホストとなるパーソナルコンピュータからのアクセスでのみ携帯情報端末のセキュリティ機能を操作管理するようにしたものである。この場合、特定の携帯情報端末のセキュリティ管理を特定のホストであるパーソナルコンピュータに限定することで携帯情報端末単体でセキュリティ機能を制御できないような仕組みを構築できる。また、携帯情報端末に機密情報を直接公開しないようにしたばかりでなく、その情報を能動的に消去することにより、不測の事態にあつても機密情報の漏洩を防止できる。また、通信機能を持つ携帯情報端末では、盗難の状況を本来の所有者に通知したり、あるいは遠隔操作でセキュリティ機能を制御することにより、より充実したセキュリティを実現できる。

【図面の簡単な説明】

【図１】本発明の実施形態を示すブロック図、

【図２】図１における記録媒体に記録されるプログラム乃至データをメモリ上に展開して示した図、

【図３】本発明の携帯情報端末の管理方法をフローチャートで示した図、

【図４】穏蔽した機密情報ファイルによる所有者情報保持方法をフローチャートで示した図、

15

【図５】不正使用を検知する方法をフローチャートで示した図、

【図６】不正使用を検知する他の方法を実現するための手順をフローチャートで示した図、

【図７】バックアップ電源を遮断することによる情報漏洩防止方法を実現するための手順をフローチャートで示した図、

【図８】強制情報削除による情報漏洩防止方法を実現するための手順をフローチャートで示した図、

【図９】強制放電による情報漏洩防止方法を実現するための手順をフローチャートで示した図、

【図１０】電子メールによる自動情報通知方法を実現するための手順をフローチャートで示した図、

【図１１】インタネット接続を通知する方法を実現するための手順をフローチャートで示した図、

【図１２】リモートアクセス認証方法を実現するための手順をフローチャートで示した図、

【図１３】セキュリティリモートコントロールの方法を実現するための手順をフローチャートで示した図、

【図１４】リモートロック方法を実現するための手順をフローチャートで示した図、

【図１５】リモート警告音発生方法を実現するための手順をフローチャートで示した図、

【図１６】リモート所在地通知方法を実現するための手順をフローチャートで示した図、

【図１７】リモートデータ消去方法を実現するための手順をフローチャートで示した図、

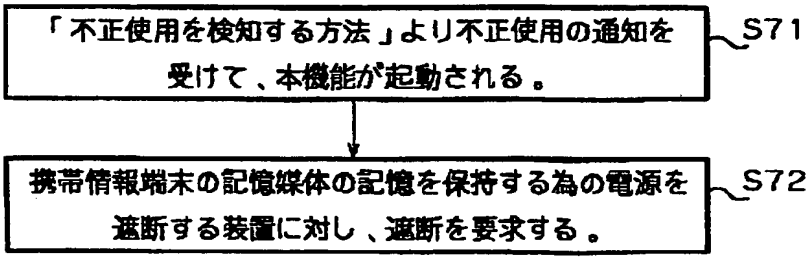
【図１８】加入電話会社から位置情報を得るための方法を実現するための手順をフローチャートで示した図、

16

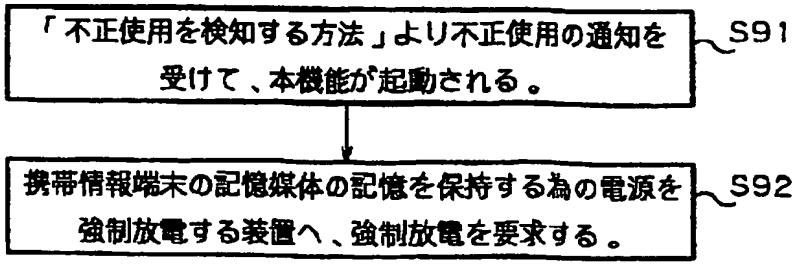
【符号の説明】

１…ホストパーソナルコンピュータ、２…電話会社（サーバ）、３…携帯情報端末、１１…記録媒体（ホスト）、３１…マイクロプロセッサ（ＣＰＵ）、３２…記録媒体（端末）、３３…不揮発性記録媒体、３４…ＰＨＳ、３５…ＧＰＳ、３６…バス、３７…バッテリ（バックアップ）、３８…強制放電装置、３９…電源遮断器、１１１…ホスト識別情報、１１２…機密情報ファイル、１１３…認識プログラム、１１４…接続情報更新プログラム、１１５…セキュリティリモートコントロールプログラム、１１６…インストーラ、１１７…位置情報取得プログラム、３２１…データ領域、３２２…プログラム領域、３２１１…機密情報ファィル、３２１２…接続情報ファイル、３２１３…個人情報ファィル、３２２１…不正使用検知プログラムＡ、３２２２…不正使用検知プログラムＢ、３２２３…電源遮断プログラム、３２２４…個人情報表示＆変更プログラム、３２２５…記録媒体強制削除プログラム、３２２６…インタネット接続検知プログラム、３２２７…自動情報通知プログラム、３２２８…パスワード要求プログラム、３２２９…強制情報削除プログラム、３２３０…リモートロックプログラム、３２３１…リモート警告音発生プログラム、３２３２…リモート所在地通知プログラム、３２３３…リモートデータ消去プログラム、３２３４…リモートアクセス認証プログラム、３２３５…インストール管理プログラム、３２３６…機密情報ファイル変更プログラム。

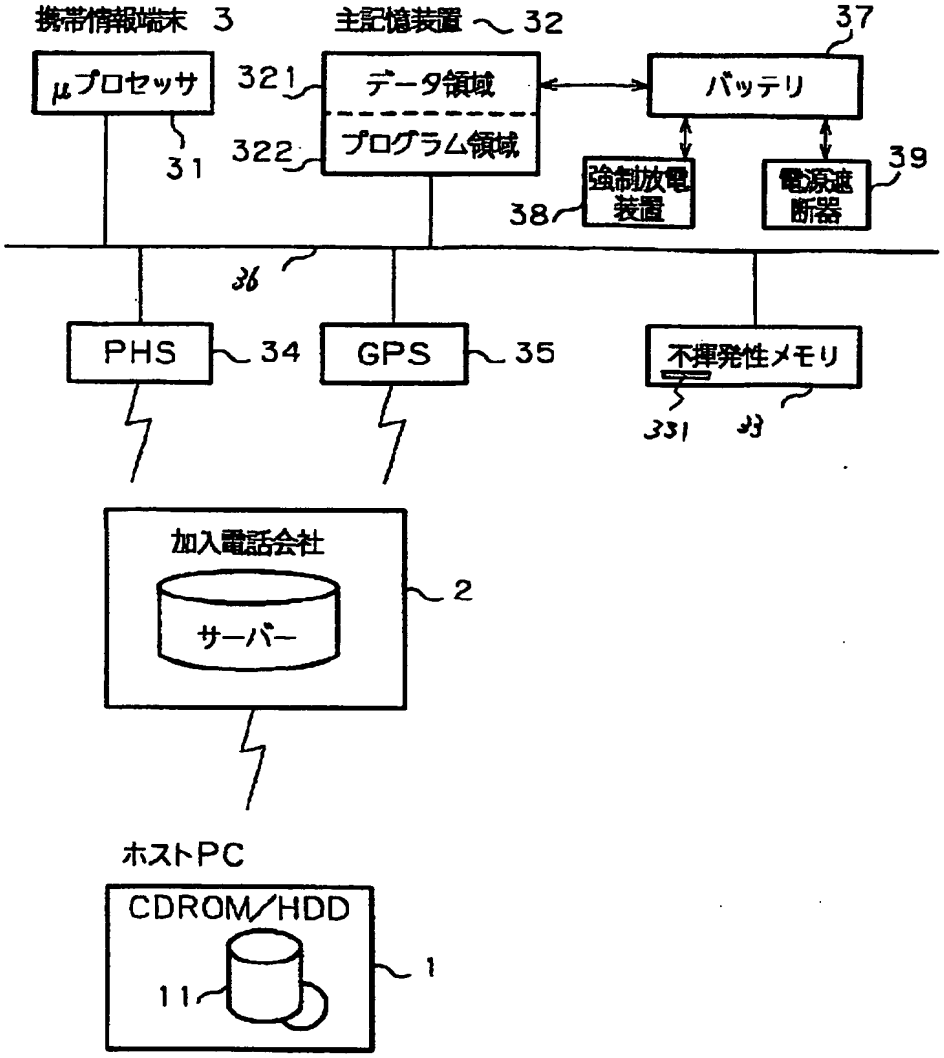
【図７】



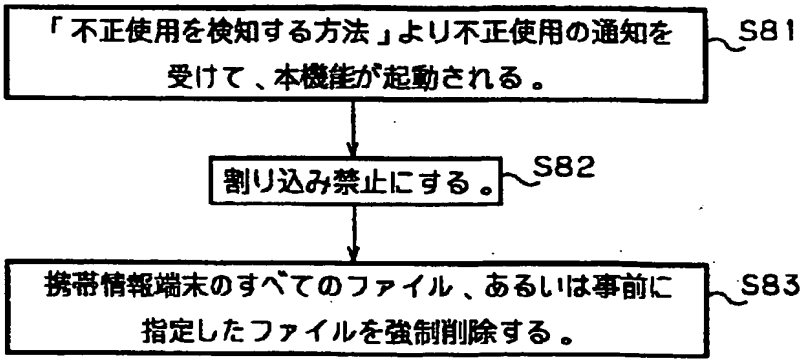
【図９】



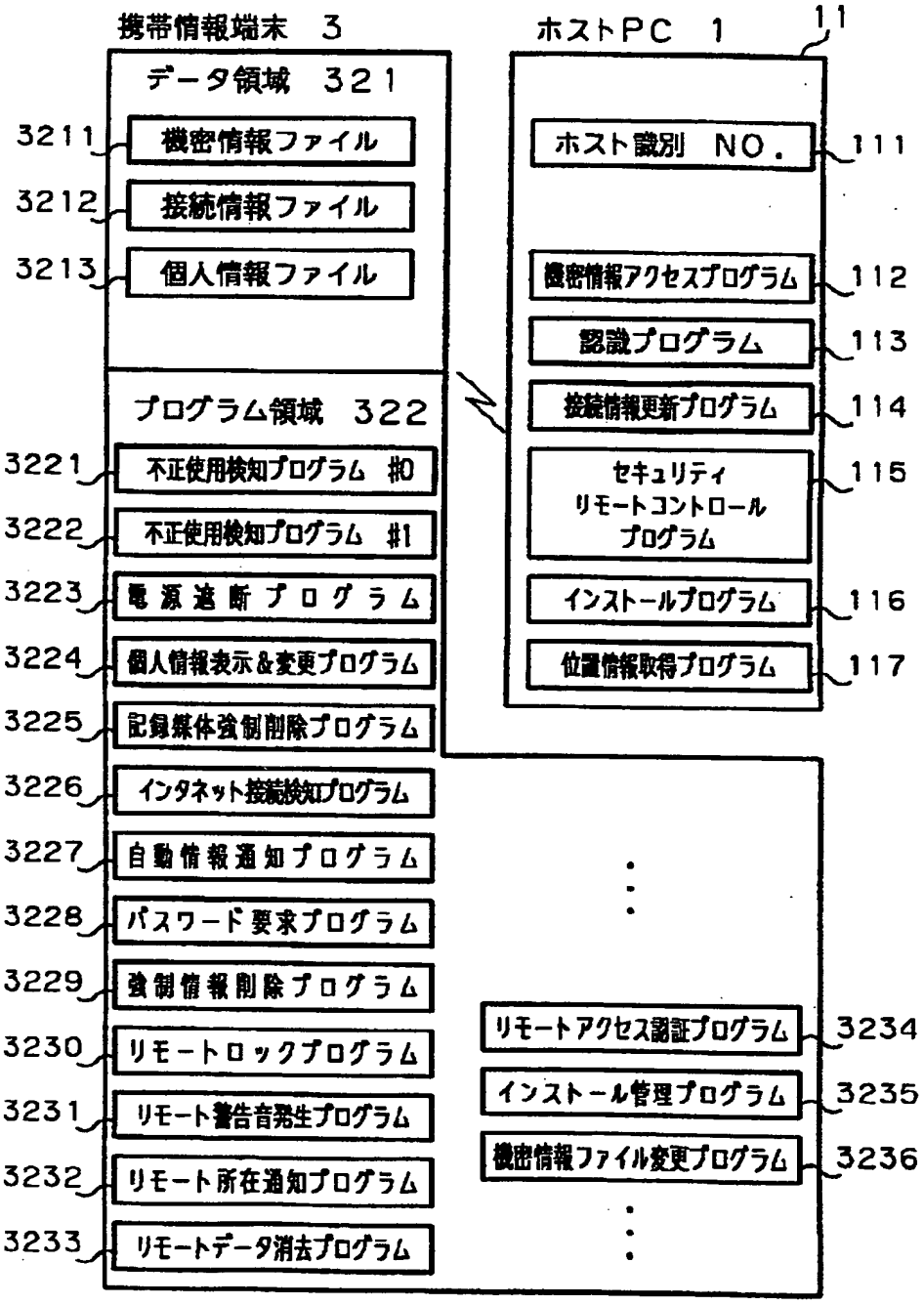
【図１】


携帯情報端末 3
主記憶装置 32
37
μプロセッサ
321
データ領域
バッテリ
31
322
プログラム領域
強制放電装置
38
電源遮断器
39
36
PHS
34
GPS
35
不揮発性メモリ
331
33
加入電話会社
サーバー
2
ホストPC
CDROM/HDD
11
1

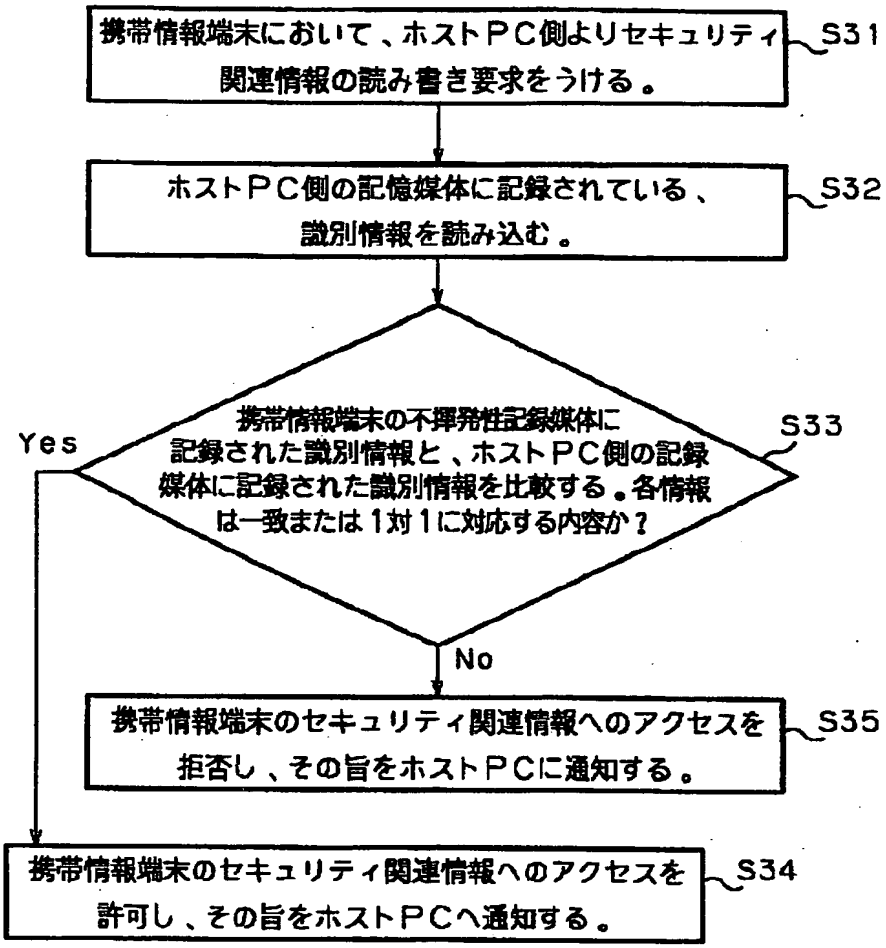
【図８】


「不正使用を検知する方法」より不正使用の通知を受けて、本機能が起動される。
S81
割り込み禁止にする。
S82
携帯情報端末のすべてのファイル、あるいは事前に指定したファイルを強制削除する。
S83

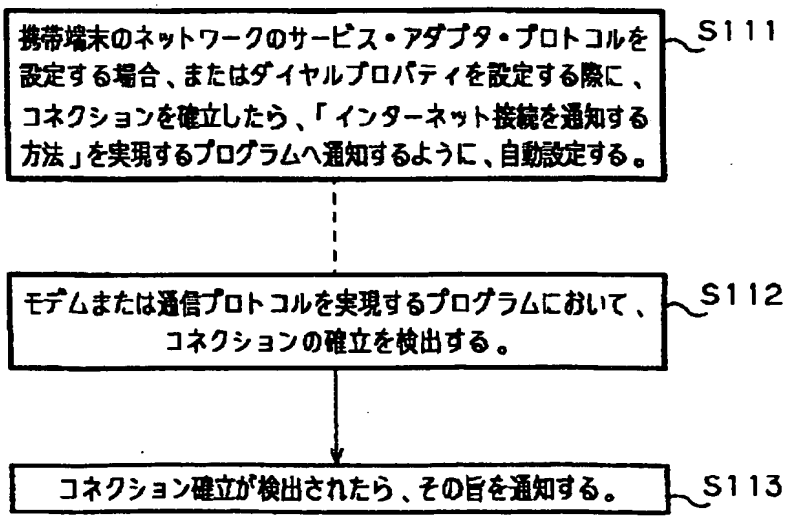
【図２】


携帯情報端末　3
データ領域　321
3211
機密情報ファイル
3212
接続情報ファイル
3213
個人情報ファイル
プログラム領域　322
3221
不正使用検知プログラム　#0
3222
不正使用検知プログラム　#1
3223
電源遮断プログラム
3224
個人情報表示&変更プログラム
3225
記録媒体強制削除プログラム
3226
インタネット接続検知プログラム
3227
自動情報通知プログラム
3228
パスワード要求プログラム
3229
強制情報削除プログラム
3230
リモートロックプログラム
3231
リモート警告音発生プログラム
3232
リモート所在通知プログラム
3233
リモートデータ消去プログラム
ホストPC　1
11
ホスト識別　NO.
111
機密情報アクセスプログラム
112
認識プログラム
113
接続情報更新プログラム
114
セキュリティ
リモートコントロール
プログラム
115
インストールプログラム
116
位置情報取得プログラム
117
リモートアクセス認証プログラム
3234
インストール管理プログラム
3235
機密情報ファイル変更プログラム
3236

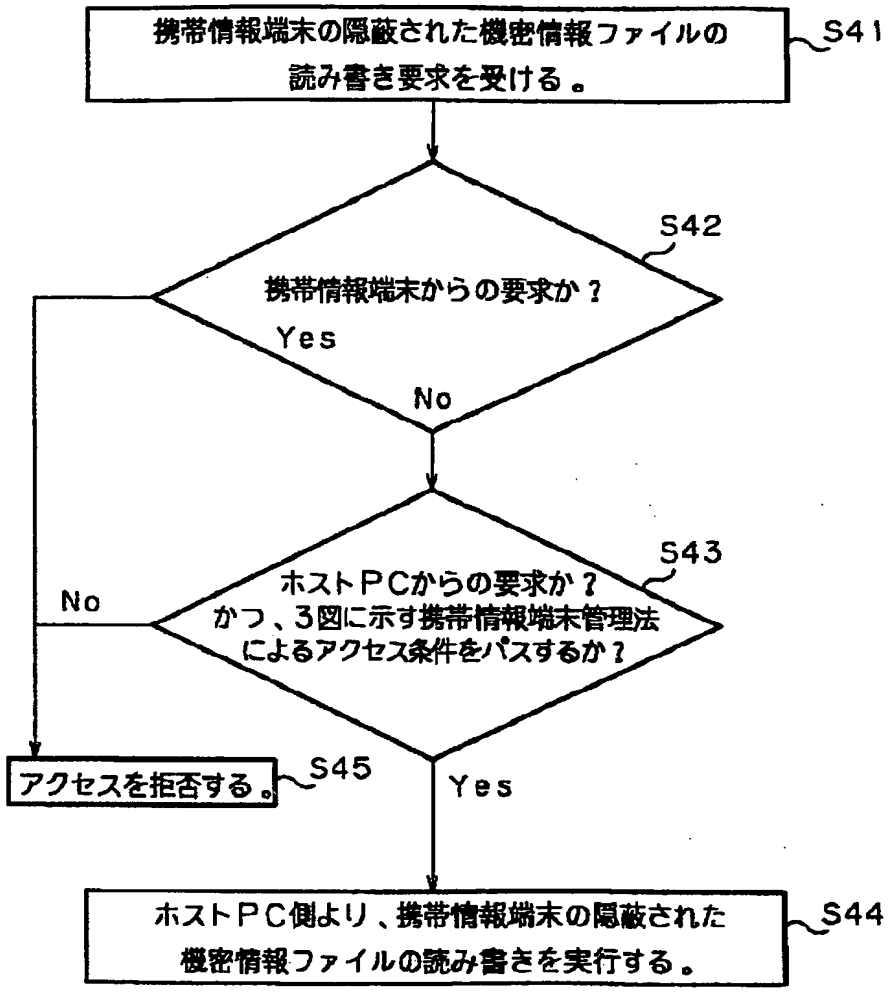
【図３】


携帯情報端末において、ホストＰＣ側よりセキュリティ関連情報の読み書き要求をうける。
S31
ホストＰＣ側の記憶媒体に記録されている、識別情報を読み込む。
S32
携帯情報端末の不揮発性記録媒体に記録された識別情報と、ホストＰＣ側の記録媒体に記録された識別情報を比較する。各情報は一致または１対１に対応する内容か？
S33
Yes
No
携帯情報端末のセキュリティ関連情報へのアクセスを拒否し、その旨をホストＰＣに通知する。
S35
携帯情報端末のセキュリティ関連情報へのアクセスを許可し、その旨をホストＰＣへ通知する。
S34

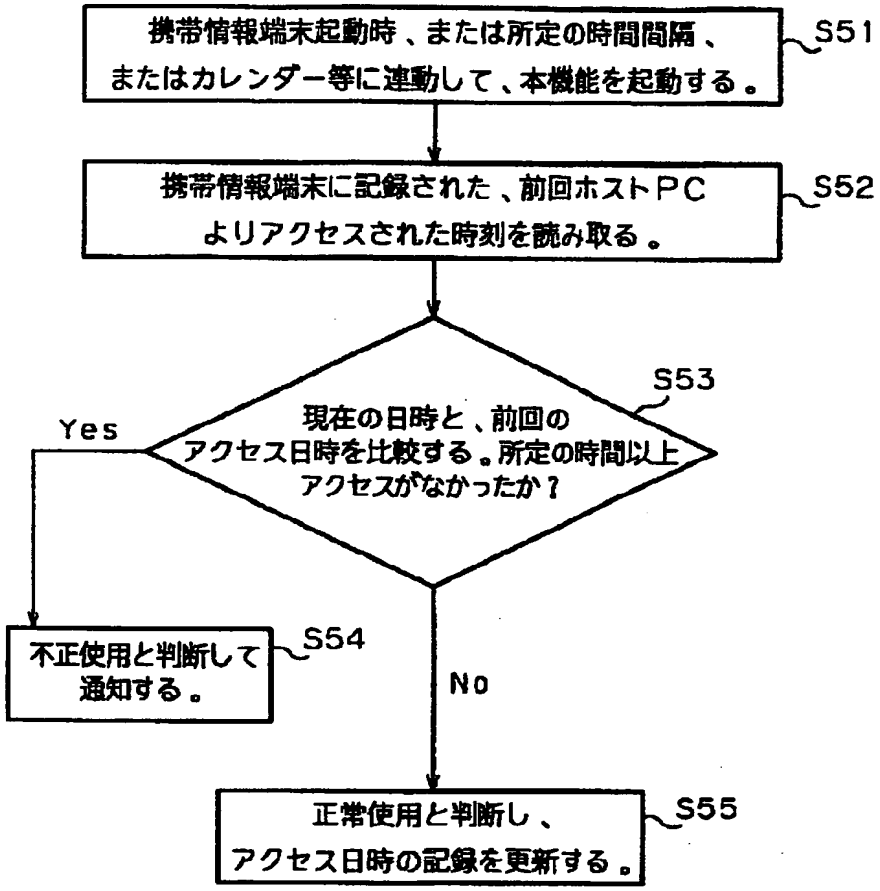
【図１１】


携帯端末のネットワークのサービス・アダプタ・プロトコルを設定する場合、またはダイヤルプロパティを設定する際に、コネクションを確立したら、「インターネット接続を通知する方法」を実現するプログラムへ通知するように、自動設定する。
S111
モデムまたは通信プロトコルを実現するプログラムにおいて、コネクションの確立を検出する。
S112
コネクション確立が検出されたら、その旨を通知する。
S113

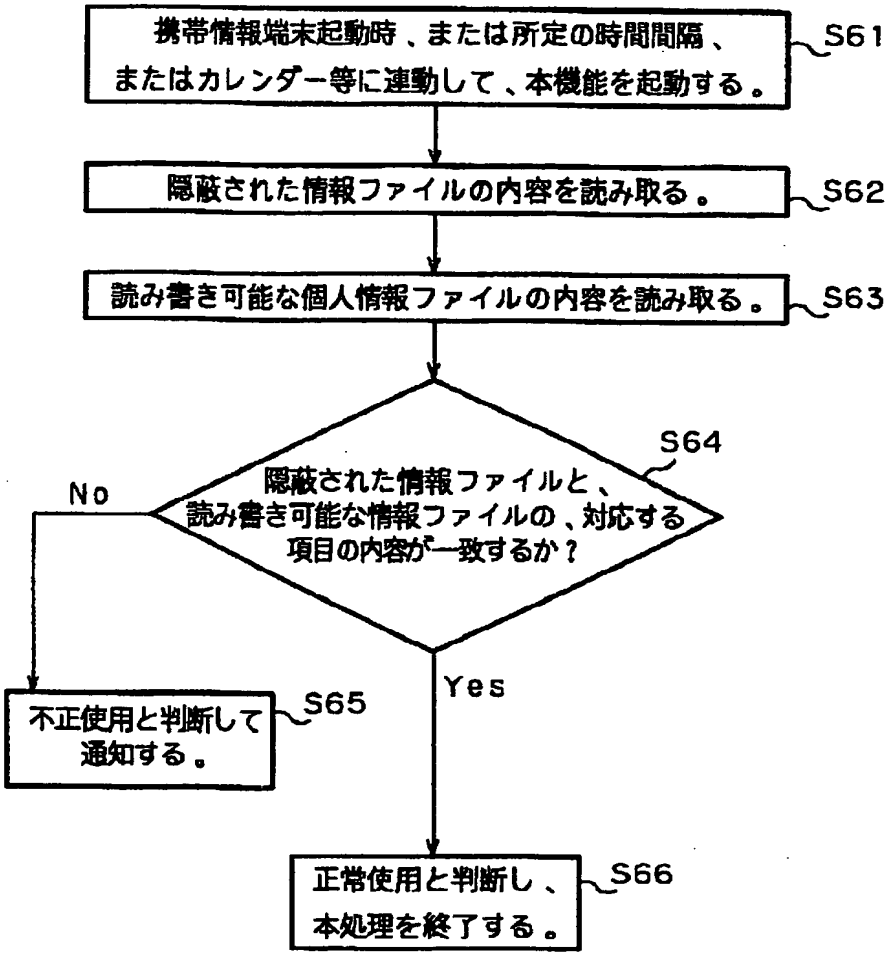
【図４】


携帯情報端末の隠蔽された機密情報ファイルの
読み書き要求を受ける。
S41
S42
携帯情報端末からの要求か？
Yes
No
S43
ホストＰＣからの要求か？
かつ、３図に示す携帯情報端末管理法
によるアクセス条件をパスするか？
No
Yes
アクセスを拒否する。
S45
ホストＰＣ側より、携帯情報端末の隠蔽された
機密情報ファイルの読み書きを実行する。
S44

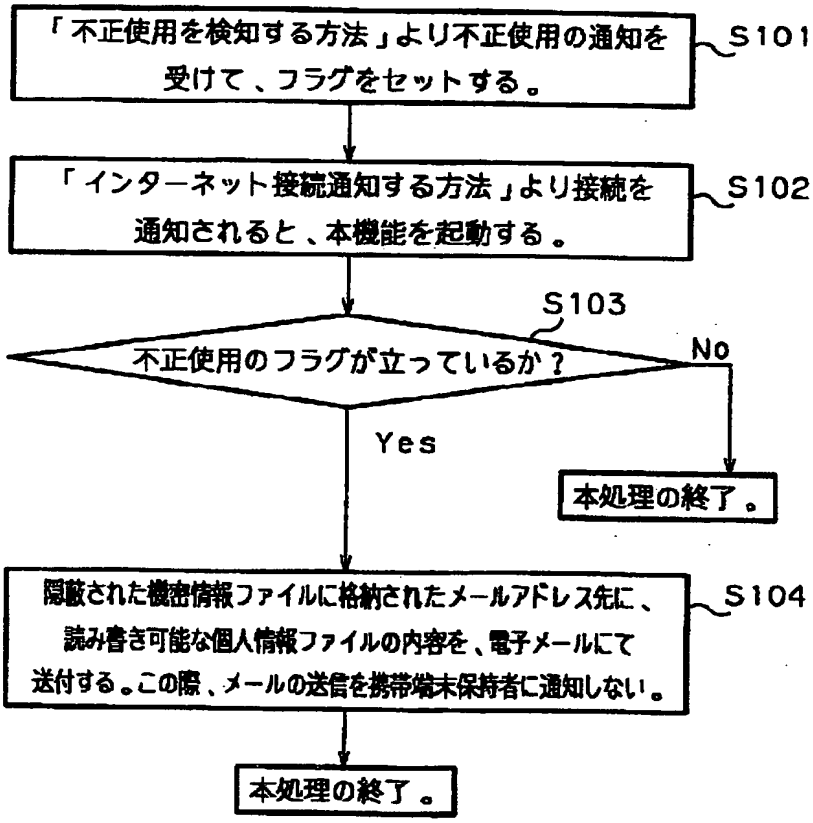
【図５】


携帯情報端末起動時、または所定の時間間隔、
またはカレンダー等に連動して、本機能を起動する。
S51
携帯情報端末に記録された、前回ホストPC
よりアクセスされた時刻を読み取る。
S52
S53
現在の日時と、前回の
アクセス日時を比較する。所定の時間以上
アクセスがなかったか？
Yes
No
不正使用と判断して
通知する。
S54
正常使用と判断し、
アクセス日時の記録を更新する。
S55

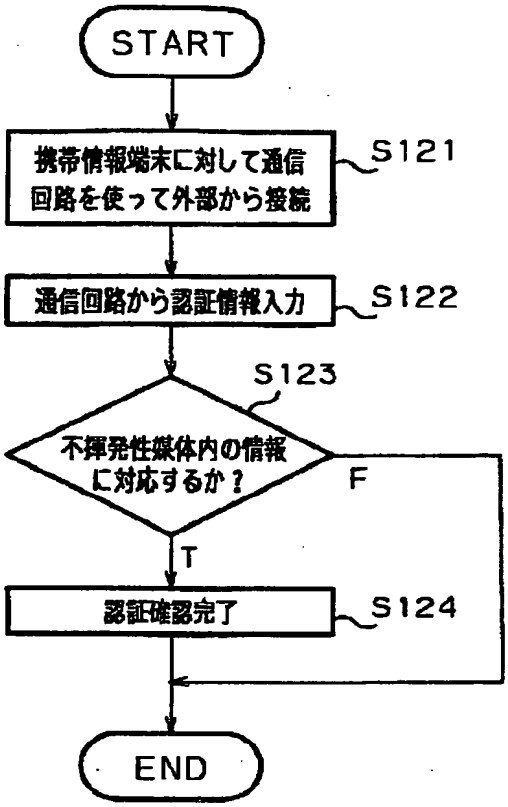
【図６】


携帯情報端末起動時、または所定の時間間隔、
またはカレンダー等に連動して、本機能を起動する。
S61
隠蔽された情報ファイルの内容を読み取る。
S62
読み書き可能な個人情報ファイルの内容を読み取る。
S63
S64
隠蔽された情報ファイルと、
読み書き可能な情報ファイルの、対応する
項目の内容が一致するか？
No
Yes
不正使用と判断して
通知する。
S65
正常使用と判断し、
本処理を終了する。
S66

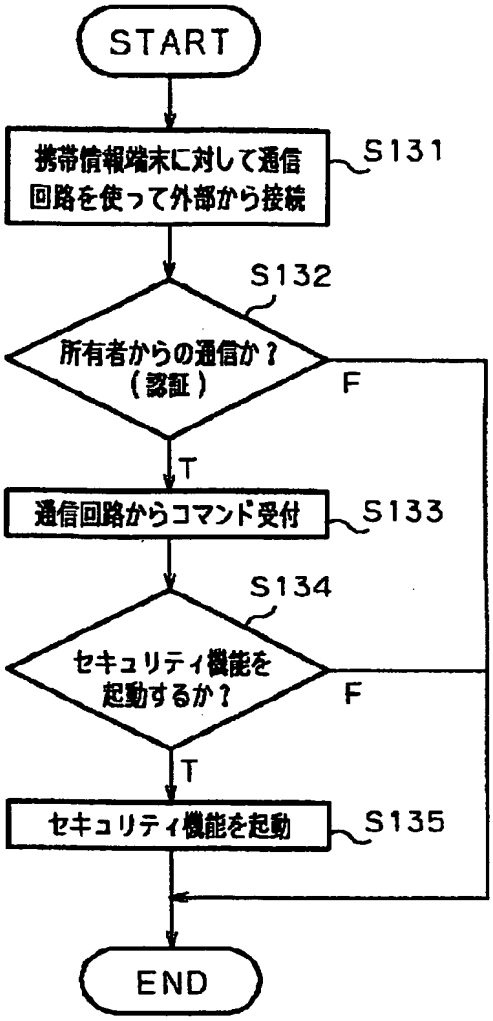
【図１０】


「不正使用を検知する方法」より不正使用の通知を受けて、フラグをセットする。
S101
「インターネット接続通知する方法」より接続を通知されると、本機能を起動する。
S102
S103
不正使用のフラグが立っているか？
No
Yes
本処理の終了。
隠蔽された機密情報ファイルに格納されたメールアドレス先に、読み書き可能な個人情報ファイルの内容を、電子メールにて送付する。この際、メールの送信を携帯端末保持者に通知しない。
S104
本処理の終了。

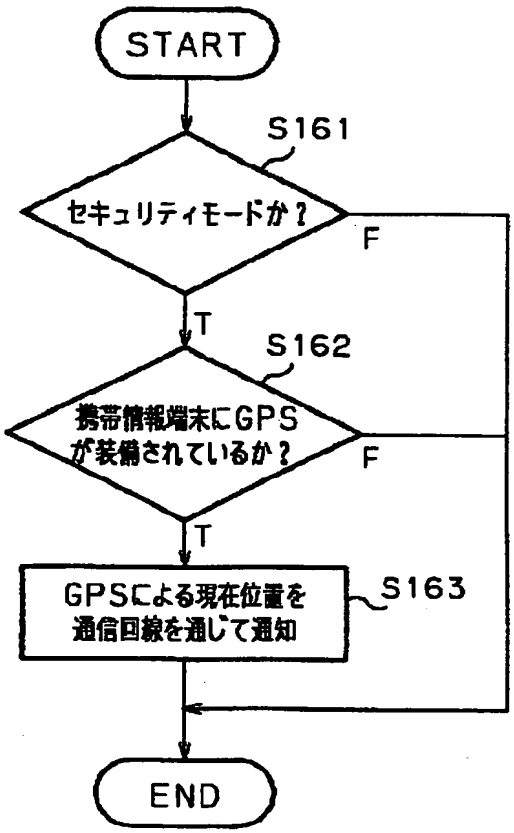
【図１２】


START
携帯情報端末に対して通信回路を使って外部から接続
S121
通信回路から認証情報入力
S122
S123
不揮発性媒体内の情報に対応するか？
F
T
認証確認完了
S124
END

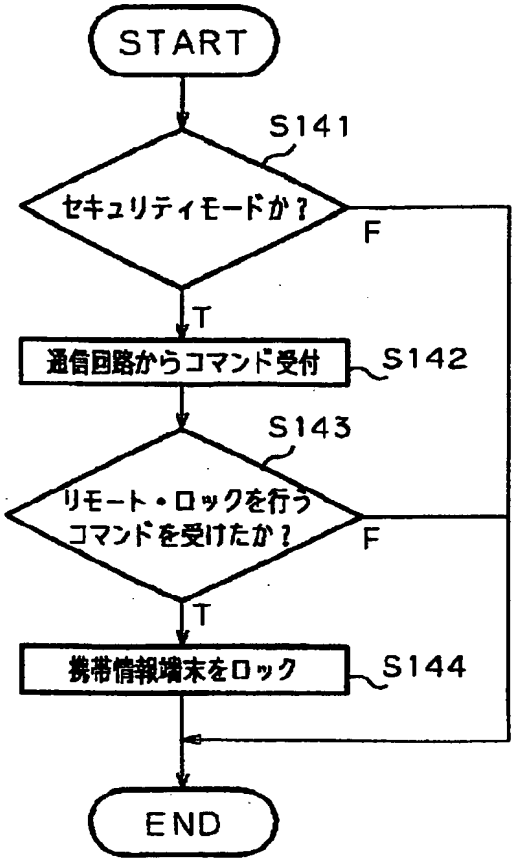
【図１３】


START
携帯情報端末に対して通信回路を使って外部から接続
S131
S132
所有者からの通信か？（認証）
F
T
通信回路からコマンド受付
S133
S134
セキュリティ機能を起動するか？
F
T
セキュリティ機能を起動
S135
END

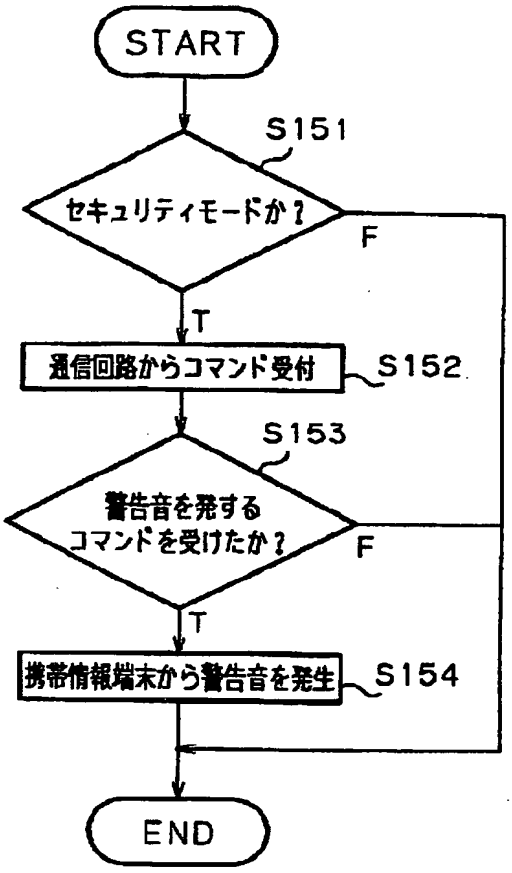
【図１６】


START
S161
セキュリティモードか？
F
T
S162
携帯情報端末にGPSが装備されているか？
F
T
GPSによる現在位置を通信回線を通じて通知
S163
END

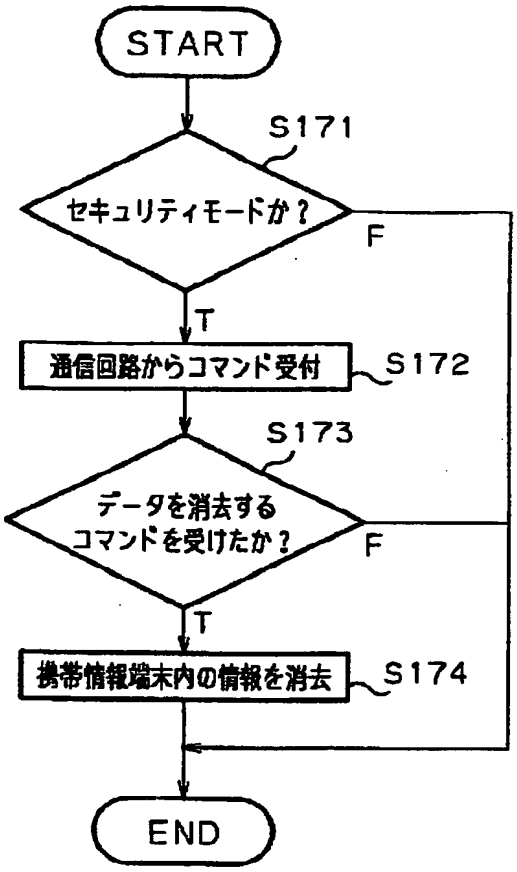
【図１４】


START
S141
セキュリティモードか？
F
T
通信回路からコマンド受付
S142
S143
リモート・ロックを行う
コマンドを受けたか？
F
T
携帯情報端末をロック
S144
END

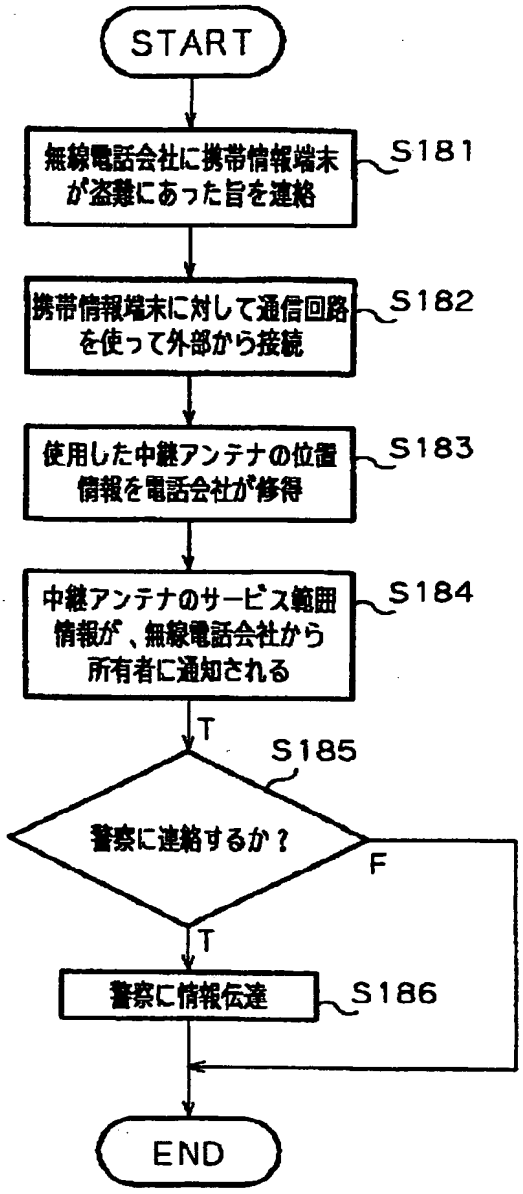
【図１５】


START
S151
セキュリティモードか？
F
T
通信回路からコマンド受付
S152
S153
警告音を発する
コマンドを受けたか？
F
T
携帯情報端末から警告音を発生
S154
END

【図１７】


START
S171
セキュリティモードか？
F
T
通信回路からコマンド受付
S172
S173
データを消去する
コマンドを受けたか？
F
T
携帯情報端末内の情報を消去
S174
END

【図１８】


START
無線電話会社に携帯情報端末が盗難にあった旨を連絡
S181
携帯情報端末に対して通信回路を使って外部から接続
S182
使用した中継アンテナの位置情報を電話会社が修得
S183
中継アンテナのサービス範囲情報が、無線電話会社から所有者に通知される
S184
T
S185
警察に連絡するか？
F
T
警察に情報伝達
S186
END